Nicolas Corry

Damian Taylor

January 2024 Edition

In this month's HORIZON:

- **Autocallables** – It started in Asia. Do we risk another global pandemic?
- **Quantum –** Are you prepared…?

Autocallables

Four years ago, the media began reporting more insistently about a respiratory illness emanating from China. Drawing on experience of how the previous Severe Acute Respiratory Syndrome (SARS) outbreak of 2003 had largely been contained within Asia, we assumed, quite wrongly, that this would be another bout of "Asian" flu.

Similarly, early in January 2024, the media has begun reporting on instances in Asia where structured products linked to China and Hong Kong indices have resulted in losses for retail investors. Regulators are looking at whether possible **mis-selling** has occurred. The kind of products which are drawing regulatory scrutiny are from a family known as autocallables. They have been sold to private clients and retail investors in Asia for years. This is because of one fundamental reason: prolonged low interest rates.

Autocallables are products which *can* provide enhanced yield (sometimes). They *can* provide capital protection (sort of). They also *can* result in the investor experiencing heavy losses (ouch!).

Autocallables are a type of product with an **asymmetric** pay off. Commonly where the underlying reference stays or appreciates above an upside strike then the product is terminated, and the investor receives a fixed yield. This is the so-called autocall. Unless the underlying reference really appreciates then the yield is likely to be superior to what could have been achieved investing in the underlying asset. Further, the fixed pay-off gives some level of certainty to the investor over what the resulting yield could be.

Where the stock falls below the upside strike, but stays above a downside strike, then the investor's capital is safe. Again, considering how this contrasts with what might have occurred investing in the underlying asset, it is plain to see that experiencing no losses is better than experiencing a loss!

Where the underlying asset fails to perform and falls below a downside trigger, then the investor tends to receive the performance of the underlying asset. In other words, all of the **losses**. This is the ouch part!

This has become a problem in Asia because of the number of products written against assets and indices in the region which have experienced dismal performance. Particularly those related to China. One such reference is the Hang Seng China Enterprises Index, which has halved over the past 5 years. But poor performance doesn't have to be so niche. The Hong Kong Hang Seng Index itself lies in negative territory so far this year, around 5%, whereas the other regional bell-weather, the Nikkei 225, is already up around 10% in 2024. In other words, a 15% underperformance…

So, why should we be concerned about an "Asian" problem?

Nicolas Corry, SKADI's MD, and a former head of CB trading, explains:

"Asian investors have proved to be an invaluable reliable hedge for credit risk. Sustained long-term low interest rates meant that it was possible for structurers to lay off credit risk for wholesale institutions by packaging it up and offering it out as enhanced yield to Asian investors. Autocallable products are a way of wholesale institutions to source volatility. Autocallable investors are selling volatility. If markets are benign, or show gains, they make money. If markets show big losses, they are exposed. What we should realise though is that, aside of the past two years, globally we have been experiencing a prolonged low interest rate cycle. It is probable that autocallables have been sold outside of Asia. It's just that in Asia, there has been recent concentrated poor performance. That hasn't happened elsewhere. Yet…."

Indeed, autocallables have been a staple of other markets outside of Asia. Switzerland is a case in point. Historically the Swiss Franc has been a lower yielding currency than its European peers. There is also a well-established private client investor base. There were some concerns regarding a popular "worst of" product late last year, when the sustained poor performance of Roche shares raised concerns investors could face losses in so called NNR products, those written on Nestlé, Novartis and Roche.

It seems probable that selling of autocallables could be widespread, with wide ranging investors seeking enhanced yields. Recent stock market performances outside of Asia, with markets hitting relative highs, has meant that it has not morphed into a problem yet. We feel there is an opportunity for control staff to get ahead of a problem that could manifest itself, if there were to be a sustained reversal in global stock market performance. And if there is one thing that is certain in 2024, it is that the outlook is uncertain.

Furthermore, particularly in the UK with its renewed focus on Consumer Duty, Regulators are paying more attention to scrutinising losses, recognising that losses can put pressure on the Financial Ombudsman Service, perhaps result in the need to make investors good by way of the Financial Services Compensation Scheme. So it seems possible that a product marketed to Retail and High Net Worth customers could draw attention should losses begin to occur.

For control staff at Wholesale Financial firms, we feel the following areas should be considered:

- Identification and quantification: How easy would it be at your institution to identify autocallables? Snowballs, lizards, cobras are just some of the catchy product names autocallables can go by. Are products tagged correctly to be recognised?
- Approvals: Given these products can often be sold to retail investors, what kinds of approval processes are followed before making an offering? Do approval processes have size thresholds, for example, which could mean that staff can bypass controls?
- Suitability: What steps are staff following to ensure they are identifying opportunities for customers which match the customer's circumstances and attitude to risk?
- Market Conformity and Price-testing: Do staff recognise that the customers being sold the product will often be unable to value the product in the same way that a wholesale structurer or trader would? What steps do staff take to ensure that pricing is fair? Where products are structured from a range of option positions, what steps do control staff take to review pricing on a relative basis within products?

Quantum – Schrödinger's rabbit

January saw the great and good on their annual trek to Davos, and the accompanying raft of headlines on issues such as AI, ESG, Basel III and cybersecurity. The reporting of one of the panel discussions caught our eye, with the headline of "is quantum going to really create a cybersecurity Armageddon?", attributed to IBM's EMEA General Manager. This, and a number of articles and research papers that we have read over the past fortnight as we disappeared down the quantum rabbit hole (Schrödinger's rabbit anyone?), has got us thinking about the post-quantum threat to financial institutions from a risk and controls perspective.

Why quantum computers represent a cyber threat to financial data

For a very brief primer on the threat to the financial sector, we turn to the opening paragraphs of a paper by the Bank for International Settlements (BIS). As their **Project Leap** paper, which looks at quantum-proofing the financial sector, describes...

"Quantum computers, should they reach sufficient size and power, may be able to break the encryption schemes widely used today to ensure secure financial transactions and data. This makes quantum computing one of the most important cybersecurity threats facing the financial system, potentially exposing all financial transactions and much of our existing stored financial data to attack.

While it is still unclear when quantum computing technology might be adopted on a large scale, its potential as a cyber threat to the financial system is already a matter of concern. Malicious actors can intercept and store confidential, classically encrypted data with the intention of decrypting it later when quantum computers become powerful enough to do so. This means that data stored or transmitted today are, in fact, exposed to "**harvest now, decrypt later**" attacks by a future quantum computer."

The legacy systems within financial institutions

Many financial firms rely on legacy systems, and much of the code underlying these is written in programming languages developed in the 1960s and 1970s like FORTRAN and COBOL (it is estimated that 90% of Fortune 500 business systems are supported by COBOL, and that 200 billion lines of COBOL code are still in use today). As banks have grown, either through mergers and acquisitions, or just through the addition of new and more complex product lines, the number of legacy systems from different generations has continued to layer on top of each other and become more and more intertwined.

The Regulatory Push

During Davos, the World Economic Forum released a White Paper, in collaboration with the FCA, entitled "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches". Much of the paper details the need for global collaboration to inform early and future regulatory approaches. The paper suggests Four Principles for Global Regulation...

- Reuse and repurpose – make best use of existing regulatory frameworks and industry practices.
- Establish non-negotiables – ensure a standardised approach to mitigating the quantum-enabled threat.
- Increase transparency – industry players must share their strategies, best practices and approaches to provide insights to regulators and other participants.
- Avoid fragmentation – avoid the potential for regulatory fragmentation across different markets and to ensure harmonised approaches.

A number of umbrella organisations within the financial services industry look to co-ordinate approaches and have also written on the quantum threat. These include, but are not limited to...

- **UK Finance** – a collective voice for the banking and finance industry, representing 300 firms across the industry.
- **The DCRF** – the Digital Regulation Cooperation Forum, that brings together the 4 UK regulators with responsibilities for digital regulation – the Competition and Markets Authority (CMA), the FCA, the Information Commissioner's Office (ICO) and Ofcom.
- **FS-ISAC** - a member-driven, not-for-profit organisation that advances cybersecurity and resilience in the global financial system. Headquartered in the US, the organization has offices in the UK and Singapore, and member financial institutions in over 70 countries.

For links to these organisation's papers and other useful information, see the end of this article. We also have a detailed repository on this (and many other topics) in the SKADI Discord – please follow this link and request access.

What to do going forward?

Whilst many think that the responsibility for quantum preparedness should sit with the CISO (Chief Information Security Officer) we believe that regulatory pushes will ensure that accountability will lie with Executive Management and the Board. Below we outline the two main priorities that we feel financial institutions should be working towards over the coming months.

Priority 1: Harvest now, decrypt later protection

There is a mind-boggling amount of data stored within financial institutions. Some of it is highly confidential (think anything client related), whilst other is less so (think pricing or transaction data). Alongside this spectrum of data confidentiality, sits a continuum of the time-sensitivity of that data. For example, modelling assumptions that are used to price up certain derivatives today are highly confidential today (and potentially very useful to competitors) but, if stolen encrypted and then decrypted in 10 years' time, of less potency. Likewise, certain data around for example, confidential Board minutes, regulatory reporting or NDAs still retain their potency many years into the future. We would therefore recommend bucketing internal data from a time-sensitivity standpoint.

Priority 2: A detailed cryptographic inventory

Whilst there (obviously) no correct prediction of when "Q-day" will come ("experts" predict from as early as 2025, whereas other cybersecurity specialists tend to think of it happening in the 2030s), what most agree is that having a full inventory of all the systems that are vulnerable to quantum computer attacks will put businesses on the front foot. As UK Finance recommends in its November 2023 paper…

"Firm Action 1: Conduct a cryptographic inventory and assessment.

Organisations should conduct a thorough inventory and assessment of their current cryptographic landscape. This process involves identifying the applications, business processes, and infrastructure that rely on cryptography and evaluating the specific cryptographic methods in use.

Understanding the existing cryptographic dependencies will help organisations identify potential vulnerabilities and prioritise updates based on risk and business requirements. This assessment will serve as the foundation for developing a tailored roadmap to transition to quantum-safe solutions."

We would recommend that control staff ensure that there is a clear understanding of where in the business this responsibility lies. Once this has been determined, we would suggest following the first 3 principles laid out by the FS-ISAC…

- Determine - What (have we got?), Where (is it?), When (was it created?), Who (owns it?), Why (are we doing it?) How (is it being used?)

- Determine what is in an organisation's control and should be inventoried and reported against.

- Determine what is outside an organisation's control and should be documented where vendors are asked to provide a risk statement, an approach for risk remediation, and roadmaps as to when changes happen that will increase agility and mitigate risk.

Useful Quantum links...

https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/

https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf?hsLang=en

https://www.drcf.org.uk/__data/assets/pdf_file/0027/262674/DRCF-Quantum-Technologies-Insights-Paper.pdf

https://www.ukfinance.org.uk/system/files/2023-11/Minimising%20the%20risks%20-%20quantum%20technology%20and%20financial%20services.pdf

Previous **Horizon** editions can be found **here**

SKADI

enquiries@skadilimited.com
www.skadilimited.com